

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (currently amended): A system for securely authenticating a data
2 exchange session with an implantable medical device, comprising:
3 a secure key repository to maintain a crypto key uniquely associated with
4 an implantable medical device to authenticate data during a data exchange
5 session; and
6 an external ~~source~~ device to establish a secure connection through a short
7 range interface with ~~[[a]] the secure key repository to securely maintain the crypto~~
8 ~~key, [[and]]~~ to authenticate authorization to access data on the implantable
9 medical device by securely retrieving the crypto key from the secure key
10 repository, and to transact the data exchange session using the crypto key to
11 authenticate the data by transitioning to a long range interface.

1 Claim 2 (cancelled).

1 3. (currently amended): A system according to ~~Claim 2~~ Claim 1,
2 further comprising:
3 an authentication component to employ the crypto key during the data
4 exchange session, comprising at least one of:
5 a command authenticator to authenticate commands exchanged
6 through the external ~~source~~ device with the implantable medical device ~~[[and ;]]~~
7 and;
8 a data integrity checker to check the integrity of the data received
9 by and transmitted from the external ~~source~~ device; and
10 a data encrypter to encrypt the data received by and transmitted
11 from the external ~~source~~ device.

1 4. (original): A system according to Claim 1, further comprising:
2 a short range interface logically defining a secured area around the
3 implantable medical device in which to establish the secure connection; and
4 a long range interface logically defining a non-secured area extending
5 beyond the secured area in which to transact the data exchange session.

1 5. (original): A system according to Claim 1, further comprising:
2 a key generator to statically generate the crypto key, and to persistently
3 store the crypto key in the secure key repository.

1 6. (original): A system according to Claim 5, wherein the crypto key
2 is stored on at least one of the implantable medical device, a patient designator, a
3 secure database, a physical token, and a repeater.

1 7. (original): A system according to Claim 5, wherein the crypto key
2 is securely retrieved from the secure key repository through a programmer.

1 8. (original): A system according to Claim 1, further comprising:
2 a key generator to dynamically generate the crypto key.

1 9. (original): A system according to Claim 8, wherein the crypto key
2 is stored on at least one of the implantable medical device, a patient designator,
3 and a repeater.

1 10. (original): A system according to Claim 8, wherein the crypto key
2 is securely retrieved from the secure key repository through at least one of a
3 programmer and a repeater.

1 11. (original): A system according to Claim 1, wherein the crypto key
2 is maintained on the implantable medical device, further comprising:
3 a short range telemetry interface retrieving the crypto key through short
4 range telemetry.

1 12. (original): A system according to Claim 11, wherein the short
2 range telemetry comprises inductive telemetry.

1 13. (currently amended): A system according to Claim 11, wherein the
2 external ~~source~~ device comprises a programmer.

1 14. (original): A system according to Claim 13, wherein the crypto key
2 is provided from the programmer to a repeater.

1 15. (currently amended): A system according to Claim 11, wherein the
2 external ~~source~~ device comprises a patient designator.

1 16. (original): A system according to Claim 15, wherein the crypto key
2 is provided from the patient designator to at least one of a programmer and a
3 repeater.

1 17. (original): A system according to Claim 1, further comprising:
2 a secure database to maintain the crypto key; and
3 a secure server providing the crypto key through a secure connection.

1 18. (original): A system according to Claim 17, wherein the secure
2 connection comprises at least one of a serial or hardwired connection and a secure
3 network connection.

1 19. (currently amended): A system according to Claim 17, wherein the
2 external ~~source~~ device comprises a programmer.

1 20. (original): A system according to Claim 19, wherein the crypto key
2 is provided from the programmer to a repeater.

1 21. (original): A system according to Claim 1, further comprising:
2 a physical token to maintain the crypto key; and
3 a reader to retrieve the crypto key by accessing the physical token.

1 22. (original): A system according to Claim 21, further comprising:

2 a physical label to specify the crypto key on the physical token.

1 23. (original): A system according to Claim 22, wherein the physical
2 label comprises at least one of alphanumeric text, bar coding, and an outwardly-
3 appearing indication.

1 24. (original): A system according to Claim 21, further comprising:
2 internal storage to specify the crypto key on the physical token.

1 25. (original): A system according to Claim 24, wherein the internal
2 storage comprises at least one of a transistor, a memory circuit, an electronically
3 readable storage medium, and a magnetically readable storage medium.

1 26. (original): A system according to Claim 21, wherein the physical
2 token is accessed using magnetic, optical, serial, and physical reading.

1 27. (original): A system according to Claim 1, wherein the crypto key
2 comprises at least one of a 128-bit crypto key and a symmetric crypto key.

1 28. (original): A system according to Claim 1, wherein the crypto key
2 comprises at least one of a statically generated and persistently stored crypto key,
3 dynamically generated and persistently stored crypto key, a dynamically
4 generated and non-persistently stored session crypto key.

1 29. (currently amended): A system according to Claim 1, wherein the
2 implantable medical device comprises at least one of an implantable cardiac
3 device, neural stimulation device, and drug therapy dispensing device.

1 30. (currently amended): A method for securely authenticating a data
2 exchange session with an implantable medical device, comprising:
3 ~~defining~~ maintaining a crypto key uniquely associated with an implantable
4 medical device in a secure key repository to authenticate data during a data
5 exchange session;

6 establishing a secure connection through a short range interface from an
7 external source ~~[[with a]]~~ with the secure key repository ~~securely maintaining the~~
8 ~~crypto key; [[and]]~~
9 authenticating authorization to access data on the implantable medical
10 device by securely retrieving the crypto key from the secure key repository; and
11 transacting the data exchange session using the crypto key to authenticate
12 the data by transitioning to a long range interface.

1 Claim 31 (cancelled).

1 32. (currently amended): A method according to ~~Claim 31~~ Claim 30,
2 further comprising:
3 employing the crypto key during the data exchange session, comprising at
4 least one of:
5 authenticating commands exchanged through the external source
6 with the implantable medical device ~~[[and ;]]~~ and;
7 checking the integrity of the data received by and transmitted from
8 the external source; and
9 encrypting the data received by and transmitted from the external
10 source.

1 33. (original): A method according to Claim 30, further comprising:
2 logically defining a secured area around the implantable medical device in
3 which to establish the secure connection; and
4 logically defining a non-secured area extending beyond the secured area in
5 which to transact the data exchange session.

1 34. (original): A method according to Claim 30, further comprising:
2 statically generating the crypto key; and
3 persistently storing the crypto key in the secure key repository.

1 35. (original): A method according to Claim 34, wherein the crypto
2 key is stored on at least one of the implantable medical device, a patient
3 designator, a secure database, a physical token, and a repeater.

1 36. (original): A method according to Claim 35, further comprising:
2 securely retrieving the crypto key from the secure key repository through a
3 programmer.

1 37. (original): A method according to Claim 30, further comprising:
2 dynamically generating the crypto key.

1 38. (original): A method according to Claim 37, wherein the crypto
2 key is stored on at least one of the implantable medical device, a patient
3 designator, and a repeater.

1 39. (original): A method according to Claim 37, further comprising:
2 securely retrieving the crypto key from the secure key repository through
3 at least one of a programmer and a repeater.

1 40. (original): A method according to Claim 30, further comprising:
2 maintaining the crypto key on the implantable medical device; and
3 retrieving the crypto key through short range telemetry.

1 41. (original): A method according to Claim 40, wherein the short
2 range telemetry comprises inductive telemetry.

1 42. (original): A method according to Claim 40, wherein the external
2 source comprises a programmer.

1 43. (original): A method according to Claim 42, further comprising:
2 providing the crypto key from the programmer to a repeater.

1 44. (original): A method according to Claim 40, wherein the external
2 source comprises a patient designator.

1 45. (original): A method according to Claim 44, further comprising:
2 providing the crypto key from the patient designator to at least one of a
3 programmer and a repeater.

1 46. (original): A method according to Claim 30, further comprising:
2 maintaining the crypto key in a secure database; and
3 retrieving the crypto key through a secure connection.

1 47. (original): A method according to Claim 46, wherein the secure
2 connection comprises at least one of a serial or hardwired connection and a secure
3 network connection.

1 48. (original): A method according to Claim 46, wherein the external
2 source comprises a programmer.

1 49. (original): A method according to Claim 48, further comprising:
2 providing the crypto key from the programmer to a repeater.

1 50. (original): A method according to Claim 30, further comprising:
2 maintaining the crypto key on a physical token; and
3 retrieving the crypto key by accessing the physical token.

1 51. (original): A method according to Claim 50, further comprising:
2 specifying the crypto key on the physical token using a physical label.

1 52. (original): A method according to Claim 51, wherein the physical
2 label comprises at least one of alphanumeric text, bar coding, and an outwardly-
3 appearing indication.

1 53. (original): A method according to Claim 50, further comprising:
2 specifying the crypto key on the physical token using internal storage.

1 54. (original): A method according to Claim 53, wherein the internal
2 storage comprises at least one of a transistor, a memory circuit, an electronically
3 readable storage medium, and a magnetically readable storage medium.

1 55. (original): A method according to Claim 50, further comprising:
2 accessing the physical token using magnetic, optical, serial, and physical
3 reading.

1 56. (original): A method according to Claim 30, wherein the crypto
2 key comprises at least one of a 128-bit crypto key and a symmetric crypto key.

1 57. (original): A method according to Claim 30, wherein the crypto
2 key comprises at least one of a statically generated and persistently stored crypto
3 key, dynamically generated and persistently stored crypto key, a dynamically
4 generated and non-persistently stored session crypto key.

1 58. (currently amended): A method according to Claim 30, wherein the
2 implantable medical device comprises at least one of an implantable cardiac
3 device, neural stimulation device, and drug therapy dispensing device.

1 59. (currently amended): An apparatus for securely authenticating a
2 data exchange session with an implantable medical device, comprising:
3 means for ~~defining~~ maintaining a crypto key uniquely associated with an
4 implantable medical device in a secure key repository to authenticate data during
5 a data exchange session;
6 means for establishing a secure connection through a short range interface
7 from an external ~~source~~ device with ~~[[a]]~~ the secure key repository ~~securely~~
8 ~~maintaining the crypto key; [[and]]~~
9 means for authenticating authorization to access data on the implantable
10 medical device by means for securely retrieving the crypto key from the secure
11 key repository; and
12 means for transacting the data exchange session using the crypto key to
13 authenticate the data by transitioning to a long range interface.

1 60. (currently amended): A system for securely transacting a data
2 exchange session with an implantable medical device, comprising:
3 a short range interface ~~to provide communication~~ device to communicate
4 with an implantable medical device by authenticating access to a securely
5 maintained crypto key using a short range interface; and
6 ~~a long range interface~~ an external device to commence a data exchange
7 session with the implantable medical device by transitioning to a long range
8 interface upon successful access authentication ~~with the implantable medical~~
9 ~~device~~, and to transact the data exchange session using the crypto key.

1 61. (original): A system according to Claim 60, wherein the patient
2 health information is maintained in an encrypted form.

1 62. (original): A system according to Claim 60, wherein the
2 authenticating with the implantable medical device is through short range
3 telemetry, further comprising:
4 a short range telemetric connection with the implantable medical device;
5 a short range telemetric device to request the crypto key from the
6 implantable medical device, and to receive the crypto key from the implantable
7 medical device.

1 63. (original): A system according to Claim 60, wherein the
2 authenticating with the implantable medical device is through a patient
3 designator, further comprising:
4 a short range telemetric connection with the implantable medical device;
5 a patient designator to request the crypto key from the implantable
6 medical device, and to receive the crypto key from the implantable medical
7 device.

1 64. (original): A system according to Claim 60, wherein the
2 authenticating with the implantable medical device is by using a physical token,
3 further comprising:

4 a physical token; and
5 a reader to receive the crypto key from the physical token.

1 65. (original): A system according to Claim 60, wherein the patient
2 health information is maintained in the implantable medical device in unencrypted
3 form and is accessible in the unencrypted form exclusively through a short range
4 telemetric connection.

1 66. (original): A system according to Claim 65, wherein the
2 authenticating with the implantable medical device is through short range
3 telemetry, further comprising:
4 a short range telemetric connection with the implantable medical device;
5 an external source to send a session crypto key to the implantable medical
6 device; and
7 an encrypter to encrypt the patient health information maintained in the
8 implantable medical device.

1 67. (original): A system according to Claim 60, wherein the
2 authenticating with the implantable medical device is through a patient
3 designator, further comprising:
4 a patient designator to establish a short range telemetric connection with
5 the implantable medical device, and to send a session crypto key to the
6 implantable medical device; and
7 an encrypter to encrypt the patient health information maintained in the
8 implantable medical device.

1 68. (original): A system according to Claim 60, wherein the long range
2 interface is augmented using one or more repeaters.

1 69. (currently amended): A method for securely transacting a data
2 exchange session with an implantable medical device, comprising:
3 maintaining a short range interface device, comprising:

4 ~~providing communication~~ communicating with an implantable
5 medical device ~~[[by]]~~; and
6 authenticating access to a securely maintained crypto key using a
7 short range interface; and
8 maintaining an external device, comprising:
9 commencing a data exchange session with the implantable medical
10 device by transitioning ~~[[to]]~~ to a long range interface upon successful access
11 authentication ~~with the implantable medical device~~; and
12 transacting the data exchange session using the crypto key.

1 70. (original): A method according to Claim 69, wherein the patient
2 health information is maintained in an encrypted form.

1 71. (original): A method according to Claim 69, wherein the
2 authenticating with the implantable medical device is through short range
3 telemetry, further comprising:
4 establishing a short range telemetric connection with the implantable
5 medical device;
6 requesting the crypto key from the implantable medical device; and
7 receiving the crypto key from the implantable medical device.

1 72. (original): A method according to Claim 69, wherein the
2 authenticating with the implantable medical device is through a patient
3 designator, further comprising:
4 establishing a short range telemetric connection between the implantable
5 medical device and the patient designator;
6 requesting for the crypto key from the implantable medical device; and
7 receiving the crypto key from the implantable medical device.

1 73. (original): A method according to Claim 69, wherein the
2 authenticating with the implantable medical device is by using a physical token,
3 further comprising:
4 accessing the physical token; and

5 receiving the crypto key from the physical token.

1 74. (original): A method according to Claim 69, wherein the patient
2 health information is maintained in the implantable medical device in unencrypted
3 form and is accessible in the unencrypted form exclusively through a short range
4 telemetric connection.

1 75. (original): A method according to Claim 74, wherein the
2 authenticating with the implantable medical device is through short range
3 telemetry, further comprising:
4 establishing a short range telemetric connection with the implantable
5 medical device;
6 sending a session crypto key to the implantable medical device; and
7 encrypting the patient health information maintained in the implantable
8 medical device.

1 76. (original): A method according to Claim 69, wherein the
2 authenticating with the implantable medical device is through a patient
3 designator, further comprising:
4 establishing a short range telemetric connection with the implantable
5 medical device through the patient designator;
6 sending a session crypto key to the implantable medical device; and
7 encrypting the patient health information maintained in the implantable
8 medical device.

1 77. (original): A method according to Claim 69, wherein the long
2 range interface is augmented using one or more repeaters.

1 78. (currently amended): An apparatus for securely transacting a data
2 exchange session with an implantable medical device, comprising:
3 means for maintaining a short range interface device, comprising:
4 means for ~~providing communication~~ communicating with an
5 implantable medical device [[by]]; and

6 means for authenticating access to a securely maintained crypto
7 key using a short range interface; and

8 means for maintaining an external device, comprising:

9 means for commencing a data exchange session with the
10 implantable medical device by means for transitioning ~~[[to]]~~ to a long range
11 interface upon successful access authentication ~~with the implantable medical~~
12 ~~device~~; and

13 means for transacting the data exchange session by accessing
14 patient health information stored on the implantable medical device using the
15 crypto key.

1 79. (currently amended): A system for securely transacting a data
2 exchange session with an implantable medical device through secure lookup,
3 comprising:

4 a secure server to provide identification of and authentication to access an
5 implantable medical device by authenticating access to a securely maintained
6 crypto key; and

7 a secure external ~~source~~ device to request the crypto key from the secure
8 server via a secure connection based on the identification of and authentication to
9 access the implantable medical device, ~~[[and]]~~ to receive the crypto key; ~~and a~~
10 ~~long range interface to,~~ to commence a data exchange session by transitioning to a
11 long range interface upon successful access authentication with the implantable
12 medical device, and to transact the data exchange session using the crypto key.

1 80. (currently amended): A method for securely transacting a data
2 exchange session with an implantable medical device through secure lookup,
3 comprising:

4 providing identification of and authentication to access an implantable
5 medical device by authenticating access to a securely maintained crypto key
6 stored on a secure server;

7 requesting the crypto key from the secure server via a secure connection
8 based on the identification of and authentication to access the implantable medical
9 device; and
10 receiving the crypto key;
11 commencing a data exchange session by transitioning [[to]] to a long
12 range interface upon successful access authentication with the implantable
13 medical device; and
14 transacting the data exchange session using the crypto key.

1 81. (currently amended): An apparatus for securely transacting a data
2 exchange session with an implantable medical device through secure lookup,
3 comprising:
4 means for providing identification of and authentication to access an
5 implantable medical device by means for authenticating access to a securely
6 maintained crypto key stored on a secure server;
7 means for requesting the crypto key from the secure server via a secure
8 connection based on the identification of and authentication to access the
9 implantable medical device; and
10 means for receiving the crypto key;
11 means for commencing a data exchange session by means for transitioning
12 [[to]] to a long range interface upon successful access authentication with the
13 implantable medical device; and
14 means for transacting the data exchange session using the crypto key.